无回显SSRF(时间判断)

中

点击保存头像,开启burpsuite抓包



可以看到avatar的一个参数,采用的是请求其他地方的图片,此时我们对这条URL进行修改

凭借dnslog并用#注释掉后面的URL地址



发现这边收到了请求



此时查看回显包发现响应的时长0.3秒

然后替换地址为127.0.0.1也就是本地的地址



发现响应的时长为1.125秒

此时依次替换为172.16.1.1和192.168.1.1

发现响应的时长都为6秒以上





也就是说我们可以用时长来判断内网中是否存在这个地址